FRAUD Insights

Fraud Insights is published by: FIDELITY NATIONAL FINANCIAL

CLICKBAIT headlines abound

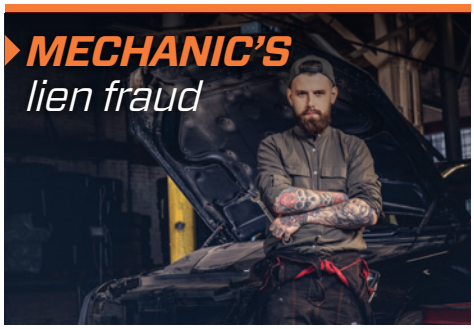
By Lisa A. Tyler
National Escrow Administrator

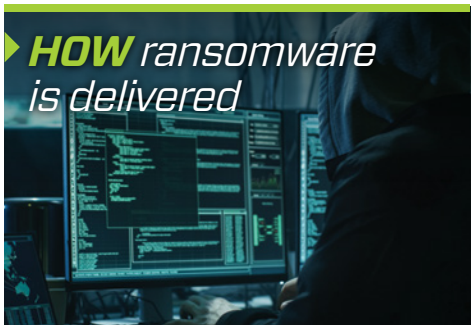
A mechanic's lien is a legal claim against a property filed by a subcontractor or material supplier when they have not received payment. The lien takes priority from the date the work began, breaking the priority of any previously recorded encumbrances. It serves as security for payment to builders, contractors and construction firms that build or repair structures. Depending on the state's statute, a mechanic's lien can be filed up to 90 or 120 days after the supplies have been bought and the work has been completed. This makes the lien dangerous. A mechanic's lien going unnoticed or unresolved can threaten real estate transactions — and even threaten a property owner's claim to the title. Clearing these types of liens is a crucial part of any real estate transaction. Read "MECHANIC'S lien fraud" for all the details.

We are frequently asked if the articles contained in this newsletter can be shared with colleagues and customers. We definitely encourage our readers to share the information contained in each edition of *Fraud Insights* through email, as well as social media. That said, in the real estate business, your integrity and reputation are everything. Fact checking and asking the important questions help keep you from sharing anything you are going to regret. We perform the fact checking for you in our newsletter, but information outside of our newsletter should be fact checked. Read "CHECK yourself: how to avoid sharing misinformation online" to manage your social media sites to your best, professional advantage.

We are continuing our 2022 series on ransomware. In order to understand how ransomware is distributed, it is important to read the article titled "HOW ransomware is delivered."

IN THIS ISSUE





Share Fraud Insights
via email, mail or word of mouth.

volume 17 issue 4
April 2022

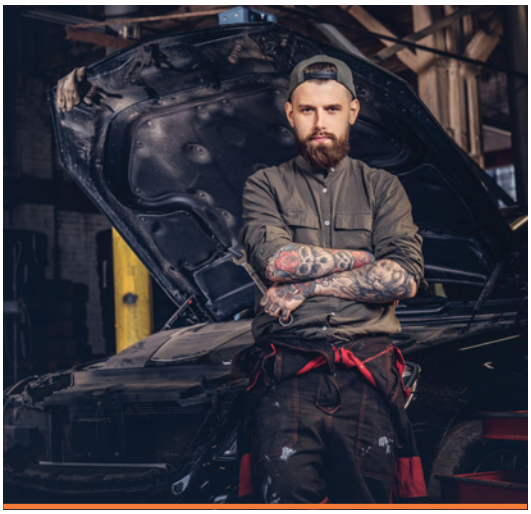
FRAUD Insights

Publisher
Fidelity National Financial

Editor
Lisa A. Tyler
National Escrow Administrator

MECHANIC'S lien fraud

A.V.P. and National Underwriter Evie Wexler of Chicago Title Insurance Company in New York, was working on title clearance for a pending transaction. The transaction involved an apartment building in Atlanta that recently underwent a remodel, which resulted in a mechanic's lien.



Evie worked with the contractor's attorney to obtain a lien release. The attorney prepared the cancellation of the lien and a demand for payment of $76,325 on behalf of his client. His demand authorized Chicago Title to record the cancellation after payment of their demand was wired.

The attorney emailed copies to Evie for her acceptance and signature. Once she signed, he agreed to overnight the original documents to her.

Evie reviewed the demand for payment and cancellation of lien. They were in order, so she signed the demand and returned it via email to the lienholder's attorney. The very next day she received a new email from the attorney which read:

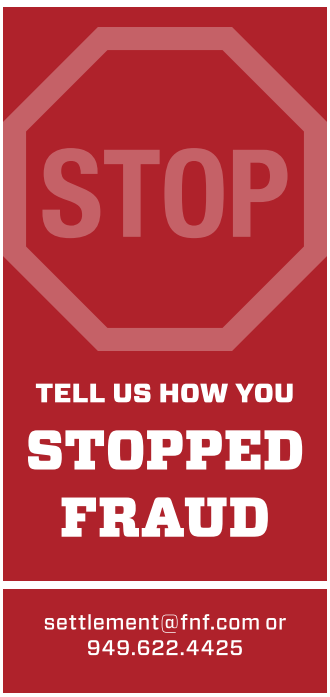
> *Good. Morning,*
>
> *Please kindly disregard the escrow letter I sent yesterday the bank Account on, I just confirm from our bank manager the account is going through financial audit and can't be able to receive or process payment during this period.*
>
> *Attached letter confirms the right accounts for payment, Please sign this so I can fedx the original today and confirm receipt of this email.*

Evie stopped dead in her tracks. She had heard about the methods used by criminals to divert wire transfers, but she could not believe it was staring her in the face. She picked up the phone and called the attorney at a known, trusted phone number she had received at the beginning of the transaction.

The attorney confirmed Evie's suspicions. He never sent her new wire instructions. Nothing was wrong with his account, and it was not being audited.

The good guys prevailed that day; but the bad guys will not stop trying. Evie knew all the signs and took the time to verify the information. Her actions saved the Company from a potential loss of nearly $77,000. For her actions, she is being rewarded $1,500. Keep up the good work!

Article provided by contributing author:
Diana Hoffman, Corporate Escrow Administrator
Fidelity National Title Group
National Escrow Administration



CHECK yourself: how to avoid sharing misinformation online

Social media sites like Facebook, Twitter, TikTok, Instagram and more give people immediate access to "news" and provide a publishing platform that is simple to use and has a wide reach.

You see a compelling story and click "share." Off that story goes to your followers and often to the public at large. Others see it, click the share button and the cycle continues.

What if that story is misleading or fake? Perhaps you determine that and delete your post. But you can't delete the shares. You've just passed along misleading information that will continue to spread across the internet.

In the real estate business, your integrity and reputation are everything. It doesn't take long to damage both, and sharing misleading information certainly does nothing to improve either. So, how does one avoid sharing misinformation in online content?

The problem
It's too easy to share. All it takes is a click or a tap and you're done. It is also quite simple not to think before clicking that share button. Then there's the sheer volume of misinformation out there along with the unreliable and far too biased sources.

Sometimes you have to wonder if there is anything out there that isn't unreliable.

Given the volume of misinformation circulating and the ease of sharing it, the best defense against spreading misinformation is self-defense.

[Continued on pg 3]

The solutions

Don't share anything. Spreading misinformation can't happen if you don't share (or create) anything. This isn't much of a solution, though. Basic human nature practically forces us to share, but "keep it to yourself" is the only foolproof solution for not sharing misleading content.

Share from reliable sources. The internet is jammed full of "news" site. Some are good, some are bad and some border on being criminal. Virtually every media site is biased from a political perspective. Skewing to the political left or right is one thing – and difficult to avoid. What should be avoided when sharing are hyperpartisan, pseudoscience and fringe/extreme sites.

An interactive media bias chart is a good place to check the bias of many "mainstream" media sites. For less popular news sites, searching Media Bias/Fact Check can tell you if a source is politically biased and/or has a history of publishing poorly fact checked material.

Fact check everything. First and foremost, everything you post or share should be fact checked. Yes, even if you're sharing directly from a reliable source. If you're sharing a news-related article, Duke University has a global directory of global fact checking sites. The Associated Press also shows its fact checking on numerous articles. If you're sharing something a user posted to social media, you cannot assume they fact checked it first.

Ask yourself who is writing what you're considering sharing and why. Are they a subject matter expert? Do they have some sort of agenda? Please note, having an agenda isn't necessarily bad, but it could mean the writer is overly biased, or not sharing both sides of the story.

Recognize your own biases. Everyone has biases. Welcome to being human. Confirmation bias, the tendency to believe what we want to believe, happens to one degree or another with everyone. Both legitimate sources and those with nefarious intentions take advantage of our confirmation bias and other biases as well. If you keep your biases in mind, you're less likely to share misinformation.

Use "STP." Stop, think, pause – before clicking the share button. Because it is so easy to share something, it's often done with little to no thought. Simply stopping your scrolling, thinking and pausing before clicking can help keep you from sharing misinformation.

Check the date of what you're sharing. While sharing something like, "Oh my, I can't believe John Doe is dead! RIP!" isn't problematic in and of itself, when you find out that Mr. Doe actually died seven years ago, you'll look rather foolish.

What will make you look even more foolish is sharing a celebrity's death notice while they are alive and well. This happens with surprising frequency and "death hoaxes" abound. In 1998, a pre-written obituary for Bob Hope was accidentally published before his death. With tears in his eyes, a Congressman announced the "death" on the floor of the U.S. House of Representatives. Of course, his speech was being shown live on national television and was subsequently picked up by all the major networks. Don't be this person.

Just stop, think, and pause before passing anything along.

Read past headlines. The web is full of glaring examples of people sharing without reading past a headline. Clickbait headlines abound in today's media; you should never share an article you haven't read.

Be aware of satire sites. Satire, a way of criticizing people or ideas in a humorous way, especially in order to make a political point, is used frequently on the internet and in social media. Entire sites are dedicated to "reporting" news using satire. While you'd think it would be stunningly obvious not to share satire as real news, it happens all the time. Just because an article is found by clicking "news" on a website doesn't make it legitimate news. STP folks, STP.

I**f you see something, say something.** Finally, if you see someone sharing misinformation, say something to them. You don't have to openly blast them; you can always send a private message. Alternatively, just be tactful in a comment. "This information isn't correct because…" or "Here's a link to an article showing the full information." Yes, it's easier to scroll by, shaking your head, but it doesn't help anyone.

Play an active role in stopping the spread of misinformation or you're almost as guilty as those spreading it.

Article provided by contributing author:
Jay Thompson
Real estate veteran and co-founder of AgentLoop living in the Texas Coastal Bend region

Originally published on February 24, 2022 on Inman.com.

FRAUD Insights

HOW ransomware is delivered

Malware needs an entry point to gain access to a computer or network. Cyber criminals continue to modify and improve their tactics, but generally they gain entry to a victim's network using one of three techniques:

1. Phishing
2. Exploiting unpatched vulnerabilities
3. Exploiting poorly secured Remote Desktop Protocols

These methods are successful, only when the victim falls for their scam. When a hacker utilizes phishing as their means of entry, the message includes an attachment or link within the body of the email that appears to be from someone the recipient already knows and trusts. This often convinces the target the document or link is safe to open.

Once the message is opened, it launches the malware that takes over their computer. The malware regularly has built-in social engineering tools that trick users into allowing administrative access. Other, more aggressive forms of ransomware, exploit software vulnerabilities to infect computers without needing to trick users.

There are several things the malware might do once it has taken over the victim's computer, but by far the most common action is to encrypt some or all of the user's files.

Ransomware hackers regularly use asymmetric encryption to lock a victim out. This type of encryption uses a public and private key — which is generated by the attacker to lock and unlock the data.

In other instances, a malicious binary file is executed, which searches for, and then encrypts, the data found on the victim's computer; the malicious binary file may also take advantage of network vulnerabilities in order to spread the malware throughout an entire organization. In either instance, the malware stays on the computer or network until its task is completed.

The files cannot be decrypted without a mathematical or decryption key known only by the attacker. The victim is presented with a message explaining their files are now encrypted and will only be decrypted if they send payment to the attacker, who usually demands some type of cryptocurrency.

The ransom must be paid within a certain amount of time, or the files will be lost forever. If a data backup is unavailable or the backups were also encrypted, the victim is faced with the difficult decision of whether or not to pay the ransom to recover personal files.

Most hackers who successfully infiltrate a computer or network not only demand a ransom — they also include a deadline. The clock starts ticking. If the victim does not pay the ransom on time, they risk losing all the data, forever.

Paying the ransom proves to be quite a quandary, since the victim knows they are dealing with thieves. Even if the victim does pay, there are no guarantees the access will be restored.

Next month's article will explore why criminals attack.

Article provided by contributing author:
Diana Hoffman, Corporate Escrow Administrator
Fidelity National Title Group
National Escrow Administration